Time Stamping Non-Repudiation And PKI

05/17/01

Mike Wolf
Chief Technical Evangelist

www.authentidate.com

AuthentiDate™
The Trusted Content Authority

Agenda

- The Company
- Goals
- What is AuthentiDate
- Why is Content Authentication important
- The need for a trusted time stamping service
- Challenges in providing trusted time
- Beyond time-stamping – the need for a 3rd party non-repudiation service
- How time stamping and non-repudiation can make PKI world a safer place
- Real World Examples of Time Stamping and Non-Repudiation in AuthentiDate's Service

AuthentiDate Corporate Overview

- Headquartered in New York City
- 26 Full Time Equivalents
- Authentidate Holding established in 1985 as BitWise Designs, NASDAQ listed as ADAT
- Authentidate established in 1999 to expand on Docstar technology to prove that scanned images had been tampered with and time of scanning

Goals

- Mission:

  Establish AuthentiDate as the leading service for authenticating and time stamping any type of electronic file that is transmitted over any type of network.

- Vision:

  Change the way world thinks about their content.

- Position:

  AuthentiDate is The Trusted Content Authority and the strongest proof that your content is original.

What is AuthentiDate

- The Authentidate solution automates the process of authenticating and time stamping any type of electronic file (such as documents, spreadsheets, pictures, video clips, audio clips, etc.) that is transmitted over any type of network.
- It uses patent pending technology that allows the user to have a trusted, non-repudiated audit trail for the electronic documents that you create, manage, or transmit.
- The audit trail is important for issues such as fraud prevention, intellectual property protection (ownership), regulatory compliance, and litigation support.

What is a Content Authority

- PKI relies on Certificate Authorities to provide root trust services for PKI infrastructures
- AuthentiDate serves as a “Trusted Content Authority” to provide content non-repudiation and time stamping for both PKI and non-PKI infrastructures

Why is Content Authentication Important for E-Business

- Digital transactions and content are inherently tamperable
- No face-to-face contact makes proving identity of parties to a transaction difficult
- PKI helps secure E-Business, but…
- Time-Stamping and Non-Repudiation can help make PKI solution 100% trustable

The Need for a Trusted Time Stamping Service

- Existing time-stamping services rely on server system clocks or at best NTP or GPS receivers
- There is no way of auditing these time stamps to prove they are accurate

Time-Stamping Challenges Facing PKI Community

- Although PKI certificates can contain a date, there is no way to prove the accuracy of the date unless a trusted time-stamping service is used
- Certificates can be signed after a signing key has expired or been revoked, and "back-dated" to make it appear they were signed when the key was valid

How time stamping and non-repudiation can make the PKI world a safer place

- By using a trusted third party time-stamping service, date field can be proven accurate
- By verifying validity of signing key at moment time stamp is applied, and storing signed certificate in a non-repudiation database, problems of “back-dating”, falsifying, tampering, or losing certificates are avoided

AuthentiDate's Time Stamping System

- Multi-Tiered architecture secured by PKI
- Atomic Master clocks at NIST audited by NIST
- Atomic Master clocks at Time Stamping Authority Audited by Master Clocks at NIST
- PKIX Time Stamp Servers at Time Stamping Authority audited by Master Clocks (FIPS-4)
- For each time stamp, auditing software can produce a "chain of trust" of time synchronization events for each time stamp applied all the way back to NIST

Challenges in commercializing PKIX time stamping

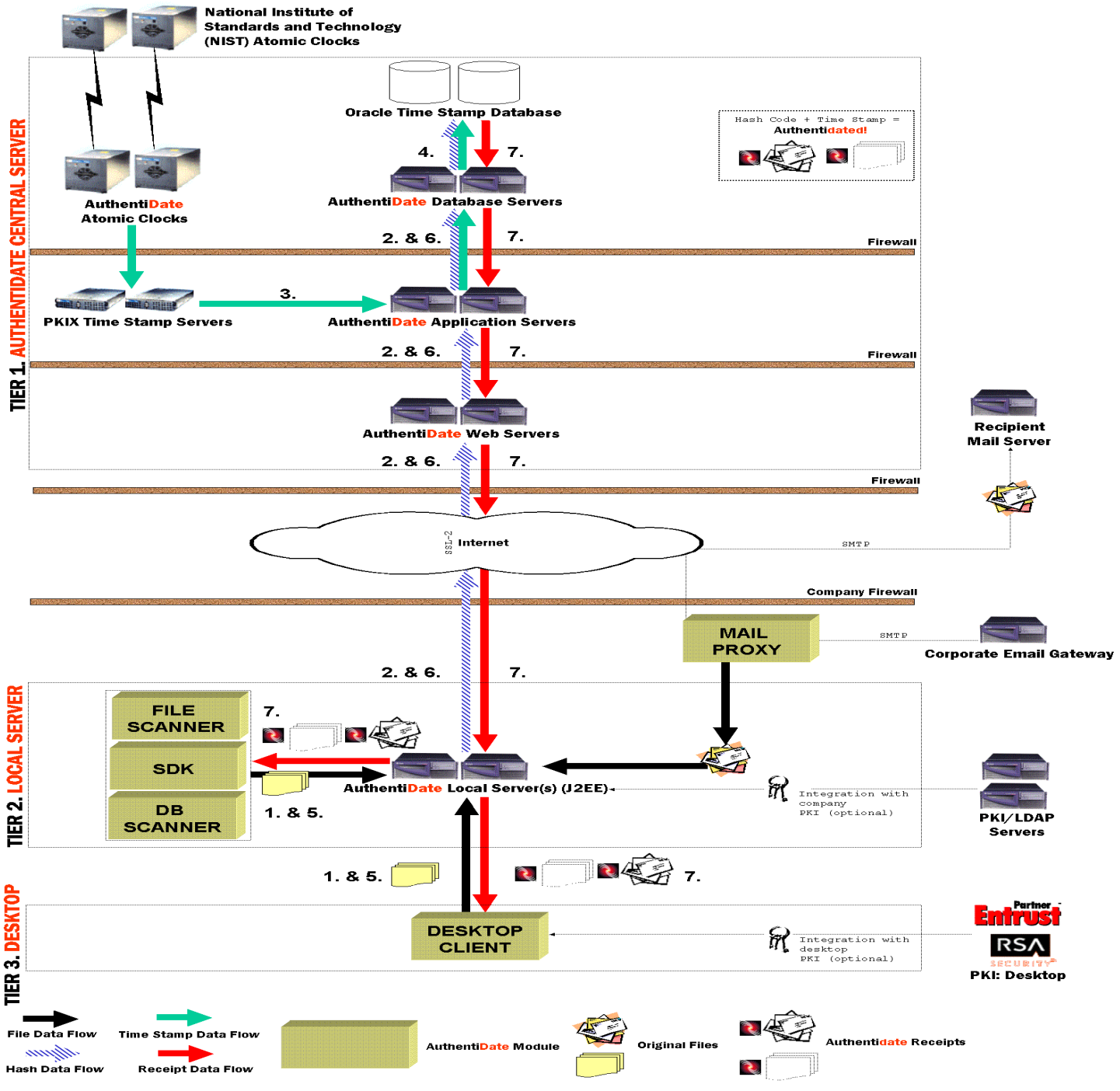
- Need to wrap user authentication and billing systems around bare PKIX time stamp protocol
- Time stamp protocol is tricky to use – requires decoding PKCS#7 certificates to get time
- Requires customer-side software to create hash codes, package them, send them, etc.

Beyond Time Stamping – the need for a 3rd Party Non-Repudiation Service

- Non-Repudiation takes time stamping to the next level of trust by storing the time-stamped transaction in a non-repudiation database
- There is an IETF draft for Non-Repudiation but it raises more questions than it answers
- No protocols defined yet for NR – defining an XML/SOAP protocol for NR should be considered by standards bodies

AuthentiDate's Non-Repudiation Service

- Sign hash code of content with server or user level certificate of customer into PKCS#7 cert which is sent to Central Server (data never leaves customer's system)
- PKIX Time Stamp server resigns hash of uploaded PKCS#7 with FIPS-Level 4 secured time-stamp with audit trail all the way to NIST for each time-stamp
- Database at Central Server stores entire transaction for later non-repudiation

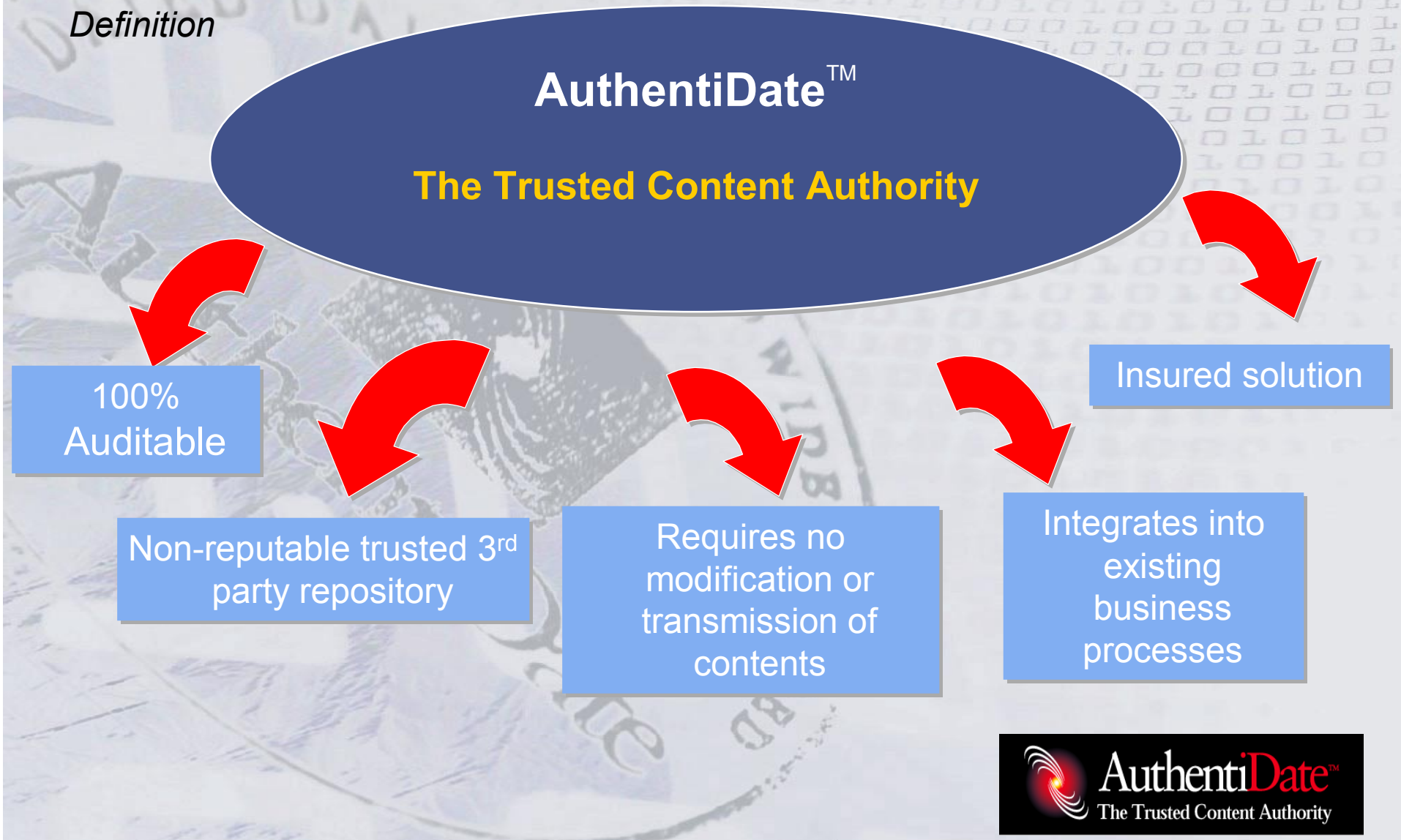

National Institute of Standards and Technology (NIST) Atomic Clocks
Oracle Time Stamp Database
Hash Code + Time Stamp = Authentidated!
AuthentiDate Atomic Clocks
4.
7.
AuthentiDate Database Servers
2. & 6.
7.
Firewall
PKIX Time Stamp Servers
3.
AuthentiDate Application Servers
2. & 6.
7.
Firewall
AuthentiDate Web Servers
2. & 6.
7.
Firewall
Recipient Mail Server
SSL-2
Internet
SMTP
Company Firewall
MAIL PROXY
SMTP
Corporate Email Gateway
2. & 6.
7.
FILE SCANNER
SDK
DB SCANNER
7.
1. & 5.
AuthentiDate Local Server(s) (J2EE)
Integration with company PKI (optional)
PKI/LDAP Servers
1. & 5.
7.
DESKTOP CLIENT
Integration with desktop PKI (optional)
Partner
Entrust
RSA SECURITY
PKI: Desktop
TIER 1. AUTHENTIDATE CENTRAL SERVER
TIER 2. LOCAL SERVER
TIER 3. DESKTOP
File Data Flow
Time Stamp Data Flow
Hash Data Flow
Receipt Data Flow
AuthentiDate Module
Original Files
Authentidate Receipts

Establishing Trust in AuthentiDate's Time Stamping and Non-Repudiation Service

- Audit by Price Waterhouse Coopers WebTrust seals for Security, Confidentiality, and Non-Repudiation
- Insurance for each transaction
- Legal opinion by Chadborne&Park that stamps are of evidentiary quality
- Escrow for stored codes for XX Years should business cease operations

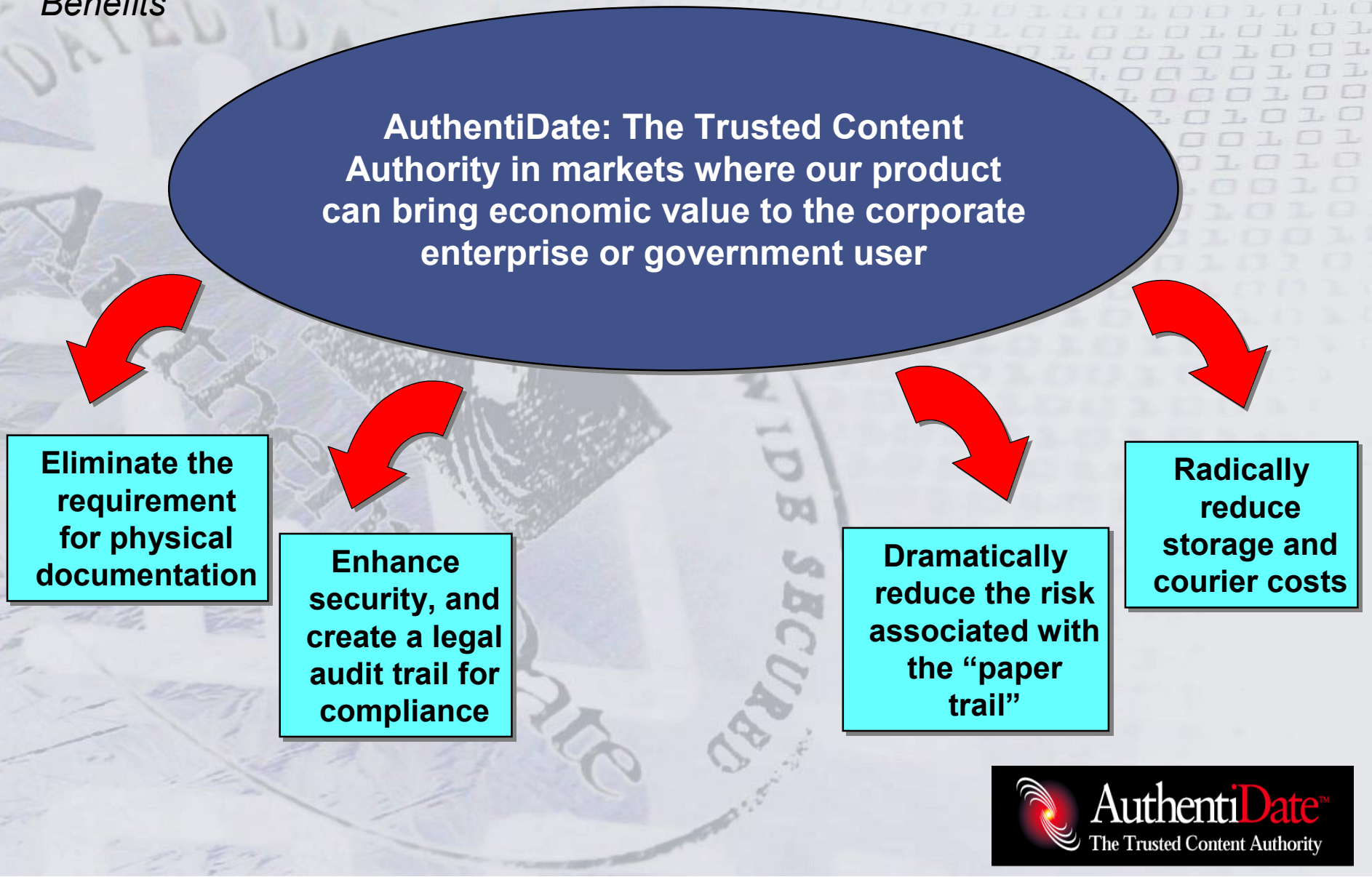
Trusted Content Authority

Definition



Trusted Content Authority

Benefits



AuthentiDate™
The Trusted Content Authority

AuthentiDate and PKI

- AuthentiDate has an internal PKI used for:
  - signing hash codes of content on customer's Local Server
  - signing time-stamps at Central Server
  - two-way SSL authentication
  - securing NTP traffic from NIST
  - signing time synchronization events

AuthentiDate and PKI if User has a PKI

- AuthentiDate is “PKI Vendor Agnostic”
- Works with RSA and Entrust PKI today
- Others to be supported
- Validates SSL and signing certificates using customer’s LDAP server
- Can sign content with user-level certificates
- AuthentiDate plus PKI proves WHO did WHAT and WHEN

AuthentiDate and PKI
If User Does NOT have PKI

- Complexities of PKI are hidden from non-PKI customer
- Content is signed with server-level certificate
- File Scanner can automatically detect creation of new files on server and AuthentiDate them automatically with no programming
- Content is protected by PKI without expense of PKI rollout
- If customer does roll out a PKI in the future, AuthentiDate can support it and do user-level signing

Thank You!
Contacts

Mike Wolf – Chief Technical Evangelist

Direct: (212) 329-1104 Cell: (518) 441-0628

Email: mwolf@authentidate.com

Barry Bergman -- VP, Sales

Direct: (212) 329-1106 Cell: (732) 616-9944

Email: bbergman@authentidate.com

Bob Zangueneh – Federal Sales Mgr

Direct: (717) 259-5707 Cell: (703) 615-6007

Email: bzangueneh@authentidate.com

AuthentiDate™
The Trusted Content Authority